REMARKS

Reconsideration and allowance of the above referenced application are respectfully requested.

Claims 10 and 33 stand rejected under 35 USC 112, second paragraph, as being depending on a canceled claim. In response, claims 10 and 33 are amended herewith for definiteness.

Claims 1, 3-6, 9, 11, 19, 21-22, 29 and 31-32 stand rejected under 35 USC 103 as allegedly being obvious over Seheidt in view of Schweitzer. This contention is respectfully traversed, and for reasons set forth herein, it is respectfully suggested that the rejection does not meet the patent office's burden of providing a prima facie showing of unpatentability.

The rejection admits that Seheidt does not teach using a nontrivial CI quasigroup to encode the information, but states that this is taught by Schweitzer. This contention is respectfully traversed.

As explained in the specification, a crossed inverse quasigroup is a special kind of quasigroup. Just teaching a quasigroup does not suggest, by itself, a crossed inverse quasigroup, and in fact a crossed inverse quasigroup has significant advantages in the context of the claimed encryption.

Any cipher system uses a key K and a message M, which are combined to produce a cipher C. Mathematically, a function exists such that F (M, K) = C.

A function that is defined by a crossed inverse quasigroup or CI quasigroup has several properties that are not found in other cipher systems. The functions defined by crossed inverse quasigroups have the following properties:

1. for every K, as M takes on all message values, the resulting values of the functions C are all distinct. (This must be true of all cipher systems if decoding is to be unique.)

2. for every M, as K takes on its key values, the resulting values of the functions see are all distinct (some cipher systems have this property and others do not).

3. There is a permutation in the key space P such that F(P(K),F(M,K))=M for all values of K and M. No other known cipher system has this property.

Properties 1 and 2 make a function a quasigroup. Some quasigroups are commutative, and some others are not. However, the property 3 distinguishes CI quasigroups from all other groups.

The CI in CI quasigroups stands for crossed inverse, and indicates the property 3, which can be explained as the mapping F(M,K)=C, which can be inverted by P(P(K),C)=M. In encoding,

the key is the second argument in the function; but in decoding, the permuted key is the first argument.

Masters does not have the properties 2 or, more importantly, 3. Masters describes matrix manipulation, which is entirely different. Nowhere is there any teaching or suggestion of a CI quasigroup in Masters, or in Seheidt for that matter.

For these reasons, each of the claims should be in condition for allowance. Claim 1 defines using a nontrivial CI quasigroup to encode the information. As described above, this is in no way taught or suggested by the cited prior art.

Claim 19 defines encrypting using a crossed inverse quasigroup, which, as described above, is not taught or suggested by the cited prior art. Claim 29 defines encrypting the message using information indicative of a crossed inverse quasigroup, and decrypting the message using the same crossed inverse quasigroup. Again, this is nowhere taught or suggested by the cited prior art.

In view of the above amendments and remarks, therefore, all of the claims should be in condition for allowance. A formal notice to that effect is respectfully solicited.

Attorney's Docket No.: 06666-032001/USC 2864

No fees are believed to be due at this time. Please apply any charges not covered or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: March 15, 2005

Scott C. Harris
Reg. No. 32,030 /BY BING AI REG. NO. 43,312

Fish & Richardson P.C.
PTO Customer Number: 20985
12390 El Camino Real
San Diego, CA 92130
Telephone: (858) 678-5070
Facsimile: (858) 678-5099
10493418.doc